AF 2134 IFW

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/931,550
Filing Date	08/16/2001
First Named Inventor	Steven Goodman
Art Unit	2134
Examiner Name	Andrew L. Nalven
Attorney Docket Number	RPS920010042
Total Number of Pages in This Submission	18

ENCLOSURES *(Check all that apply)*

- ☑ Fee Transmittal Form
  - □ Fee Attached
- □ Amendment/Reply
  - □ After Final
  - □ Affidavits/declaration(s)
- □ Extension of Time Request
- □ Express Abandonment Request
- □ Information Disclosure Statement
- □ Certified Copy of Priority Document(s)
- □ Reply to Missing Parts/ Incomplete Application
  - □ Reply to Missing Parts under 37 CFR 1.52 or 1.53

- □ Drawing(s)
- □ Licensing-related Papers
- □ Petition
- □ Petition to Convert to a Provisional Application
- □ Power of Attorney, Revocation Change of Correspondence Address
- □ Terminal Disclaimer
- □ Request for Refund
- □ CD, Number of CD(s) ____________
  - □ Landscape Table on CD

- □ After Allowance Communication to TC
- □ Appeal Communication to Board of Appeals and Interferences
- ☑ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- □ Proprietary Information
- □ Status Letter
- ☑ Other Enclosure(s) (please Identify below):

Return Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Winstead Sechrest & Minick P.C.		
Signature			
Printed name	Kelly K. Kordzik		
Date	11-17-05	Reg. No.	36,571

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Toni Stanley		
Typed or printed name	Toni Stanley	Date	11-17-05

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/17 (11-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 10/01/2004. Patent fees are subject to annual revision.

FEE TRANSMITTAL
For FY 2005

□ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500.00

Complete if Known	
Application Number	09/931,550
Filing Date	08/16/2001
First Named Inventor	Steven Goodman
Examiner Name	Andrew L. Nalven
Art Unit	2134
Attorney Docket No.	RPS920010042

METHOD OF PAYMENT (check all that apply)

□ Check □ Credit Card □ Money Order

☑ Deposit Account □ None

Deposit Account Number: 50-3533
Deposit Account Name: Lenovo, Inc.

The Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below
□ Charge fee(s) indicated below, **except for the filing fee**
☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17
☑ Credit any overpayments

to the above–identified deposit account.

□ Other (please identify):____________

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING FEE

Fee Description	Fee ($)	Small Entity Fee ($)	Fee Paid($)
Utility Filing Fee	790	395	
Design Filing Fee	350	175	
Plant Filing Fee	550	275	
Reissue Filing Fee	790	395	
Provisional Filing Fee	160	80	

Subtotal (1) $__________

FEE CALCULATION (continued)

2. EXTRA CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20	50	25
Each independent claim over 3	200	100
Multiple dependent claims	360	180
For Reissues, each claim over 20 and more than in the original patent	50	25
For Reissues, each independent claim more than in the original patent	200	100

Total Claims ______ - 20 or HP = **Extra Claims** ______ x **Fee ($)** ______ = **Fee Paid ($)** ______
HP = highest number of total claims paid for, if greater than 20

Indep. Claims ______ - 3 or HP = **Extra Claims** ______ x **Fee ($)** ______ = **Fee Paid ($)** ______
HP = highest number of independent claims paid for, if greater than 3

Multiple Dependent Claims **Fee ($)** ______ **Fee Paid ($)** ______

Subtotal (2) $__________

3. OTHER FEES

Fee Description	Fee ($)	Small Entity Fee ($)	Fee Paid($)
1-month extension of time	120	60	
2-month extension of time	450	225	
3-month extension of time	1,020	510	
4-month extension of time	1,590	795	
5-month extension of time	2,160	1,080	
Information disclosure stmt. fee	180	180	
37 CFR 1.17(q) processing fee	50	50	
Non-English specification	130	130	
Notice of Appeal	500	250	
Filing a brief in support of appeal	500	250	500
Request for oral hearing	1,000	500	
Other:__________			

Subtotal (3) $ 500

SUBMITTED BY			
Signature		Registration No. (Attorney/Agent) 36,571	Telephone 512.370.2851
Name (Print/Type)	Kelly K. Kordzik		Date 11-17-05

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Goodman et al.	:	Before the Examiner: Nalven, Andrew L.
Serial No.: 09/931,550	:	Group Art Unit: 2134
Filing Date: August 16, 2001	:	
Title: SYSTEM MANAGEMENT INTERRUPT GENERATION UPON COMPLETION OF CRYPTOGRAPHIC OPERATION	:	Lenovo (United States) Inc. ZHHA/B675/B424 P.O. 12195 3039 Cornwallis Road Research Triangle Park, NC 27709

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. REAL PARTY IN INTEREST

Lenovo (Singapore) Pte. Ltd. is the assignee of the entire right, title and interest in the above-identified patent application.

CERTIFICATION UNDER 37 C.F.R. §1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on 11-17, 2005.

Toni Stanley
Signature

Toni Stanley
(Printed name of person certifying)

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, Appellants' legal representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 3-9 and 12-19 are pending in the Application. Claims 3-9 and 12-18 stand rejected. Claim 19 is allowed.

IV. STATUS OF AMENDMENTS

Appellants have not submitted any amendments following receipt of the final rejection with a mailing date of July 28, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is described with respect to the update of a BIOS image within a data processing system, such as system 413 shown in FIGURE 4. However, the present invention is applicable to the update of any data and/or image within an information handling system. Page 8, lines 17-19.

The present invention makes use of the TCPA (Trusted Computing Platform Alliance) Specification where a trusted platform module (TPM) 451 has been installed within system 413. The TCPA Specification is published at www.trustedpc.org/home/home.htm, as version 1.0, which is hereby incorporated by reference herein. However, it should be noted that the present invention may also be implemented using other cryptographic verification methods and processes. Page 8, lines 20-25.

Referring to FIGURE 1, system 413, either automatically, or as a result of input from a user, will begin a process where the BIOS image is to be updated. In step 101, the process of the present invention will initially request an unlock of the

BIOS image from an SMI handler. FIGURE 2 illustrates a process for implementing such an SMI handler in accordance with the present invention, wherein step 201, the BIOS update application (flash utility) requests a flash unlock from the SMI handler. Page 9, lines 1-8.

A receipt of an SMI causes the system to enter into a mode referred to as system management mode (SMM). SMIs can be asserted by an SMI timer, by a system request, or by other means, such as an application. An SMI is a non-maskable interrupt having almost the highest priority in the system 413. When an SMI is asserted, CPU 410 maps a portion of memory referred to as the system management mode memory (SMM memory) into the main memory space (e.g., RAM 414). The entire CPU 410 state is then saved in the SMM memory in stack-like, last in/first out fashion. After the initial processor state is saved, CPU 410 begins executing an SMI handler routine, which is an interrupt service routine typically performing system management tasks such as reducing power to specific devices or, as in the case of the present invention, providing a secure means for updating a flash utility. While the routine is executing, other interrupt requests are not serviced, and are ignored until the interrupt routine is completed or the CPU 410 is reset. When the SMI handler completes its task, the processor state is retrieved from the SMM memory, and the main program continues. Page 9, lines 9-22.

In step 203, an SMI handler requests cryptographic signature verification from the TPM 451 and sets a status code as Pending. The process in FIGURE 2 will then proceed to step 204, where the SMI handler exits and returns the Pending status to the BIOS update application of FIGURE 1. In FIGURE 1, it is at this point that the process will proceed to step 102, where the Pending status set in step 203 is received from the SMI handler, and since the status code is set as Pending, in step 103, the process of FIGURE 1 will loop back to step 101. Page 9, line 23- page 10, line 5.

While this is occurring, step 203 has caused the initiation of the process in FIGURE 3. In step 301, the TPM 451 issues an SMI upon completion of a verification request (step 203) and an SMI handler queries the TPM 451 for the status of such cryptographic verification process. The TPM 451 may utilize a signature verification process that is a standard method that is used in many cryptographic systems. The sender of the BIOS image computes a "hash" of the original work (a hash is a mathematical computation that is performed on the input; the computation is designed such that the probability of being able to recreate the output without the identical input is low). Then the hash is encrypted using the sender's private key. This encrypted result is called the signature. When the receiver, the TPM 451, wishes to verify that the image is authentic, the TPM 451 computes the hash of what was received. The TPM 451 then decrypts the sender's signature by using the sender's public key and compares it to the newly computed hash. If they are identical, the TPM 451 then determines that the update image is authentic and has not been modified in transit. Page 10, lines 6-19.

Next, assume that the verification process in step 301 has completed, and the TPM has determined that the BIOS update image received by system 413, such as through network 450, or on a diskette, has resulted in a verification that the image is authentic. As a result, the process in FIGURE 3 will proceed from step 302 to step 303 to set the status as Successful. Page 11, lines 4-8.

The SMI handler will now unlock the flash memory to allow the update of the BIOS image and the SMI handler sets the status as a successful completion. In step 204, the SMI handler exits and returns the process to step 102 in FIGURE 1. Since the status is no longer Pending, the process proceeds from step 103 to step 104. The status being Successful, the process proceeds to step 105, where the BIOS has been updated, and the SMI handler is now called to lock the flash memory. Page 11, lines 13-19.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 3-9 and 12-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Alexander et al.* (U.S. patent No. 6,188,602) in view of *Grawrock* (U.S. Patent No. 6,678,833).

VII. ARGUMENT

Claims 4-6, 13-15 and 18 stand rejected under 35 U.S.C. § 103 as being unpatentable over *Alexander* in view of *Grawrock* (U.S. Patent No. 6,678,833). In response, Applicants respectfully traverse these rejections.

The Examiner is attempting to combine *Grawrock* and *Alexander* in an impermissible manner. Nothing within *Alexander* teaches or suggests a need or even a hint for using a TPM such as taught in *Grawrock.*

The Examiner asserts that the motivation to combine the two references is provided in *Grawrock* at column 2, lines 1-6. *Grawrock* teaches that the TPM is bound physically or logically to the boot block memory device, such as shown in Figure 2 of *Grawrock.* This resulting configuration allows the TPM to accurately report the identity of the boot block without reliance on any intervening devices. Though a combination of *Grawrock* and *Alexander* may suggest that a TPM can be used to verify the identity of a boot block code, it does not suggest an ability to use a TPM to verify and update to such a boot block code, or especially a BIOS utility, such as recited in some of the claims. In fact, *Grawrock* teaches away from the present invention by specifically stating that it uses the TPM so that there is no reliance on any intervening devices, while the present invention uses such an intervening device through the utilization of the SMI handler to query a status of the verifying step. In other words, *Grawrock* has the TPM so physically or logically connected to the boot block memory unit that it does not require such utilities as an SMI handler to assist it in verifying updates that may be desired to be stored on such a memory unit. The Examiner responds that an SMI handler is not a "device." It appears the Examiner is taking an overly narrow interpretation of the term "device," contrary to normal PTO practice.

With respect to claims 5 and 14 the Examiner asserts that the combination of *Alexander* and *Grawrock* would teach that an SMI handler could be used to query the status of the verifying step by querying the TPM for such status. The Examiner cites *Grawrock*, column 4, lines 1-9. This language in *Grawrock*, however, teaches that the TPM can be used to perform a hash operation on various software modules to produce an identifier that is then stored within the TPM, and then can be used to later respond to challengers wanting to verify the authenticity of such software modules. Column 3, line 50 - column 4, line 18. What is important is that the combination of these two references does not teach or suggest that an update to one of these software modules, and specifically the BIOS (as recited in several of the claims), is performed by the TPM before an update of such software module is accomplished. *Grawrock* teaches verification after it has already been loaded onto the system, whereas the present invention teaches a way to verify the BIOS is unaltered before allowing it to be flashed onto the system. This is the same difference as between catching the criminal after the crime has been committed versus preventing the crime.

Column 5, lines 41-45, does not teach "if the verifying step successfully verifies the update of the utility, unlocking the utility and updating the utility." The "unlocking" step is missing in *Alexander's* disclosure. And, yes, the claims do recite that verification must be completed. That is what "successfully verifies" means.

With respect to claims 6 and 15, the Examiner has asserted that the combination of *Alexander* and *Grawrock* teaches the SMI handler being issued by the TPM. This is in no way suggested by these two combinations. The Examiner cannot make such an assertion without attempting to at least prove it with some logical reasoning. The Examiner's assertion on page 5 of the Office Action is merely an unsupported single-sentenced statement.

With respect to claim 18, the foregoing arguments also apply.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Appellants

By:__________________________________
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2832

CLAIMS APPENDIX

3. The method as recited in claim 4, further comprising the step of:

not unlocking the utility if the verifying step fails to verify the update to the utility.

4. In a data processing system, a method for updating a utility, comprising the steps of:

receiving a request to unlock the utility;

verifying an update to the utility;

using a system management interrupt (SMI) handler to query a status of the verifying step;

and

if the verifying step successfully verifies the update of the utility, unlocking the utility and updating the utility, wherein the verifying step is performed by a trusted platform module (TPM) in accordance with Trusted Computing Platform Alliance Specifications.

5. The method as recited in claim 4, wherein the SMI handler used to query the status of the verifying step queries the TPM for the status.

6. The method as recited in claim 5, wherein the SMI handler is issued by the TPM.

7. The method as recited in claim 4, further comprising the step of:

after the utility has been updated, locking the utility with the SMI handler.

8. The method as recited in claim 4, wherein the utility is a flash utility.

9. The method as recited in claim 4, wherein the requesting step is performed by an SMI handler.

12. The computer program product as recited in claim 13, further comprising:

programming for not unlocking the utility if the verifying programming fails to verify the update to the utility.

13. A computer program product for storage on a computer readable medium and operable for updating a utility, comprising:

programming for receiving a request to unlock the utility;

programming for verifying an update to the utility;

programming for using a system management interrupt (SMI) handler to query a status of the verifying programming; and

if the verifying programming successfully verifies the update of the utility, programming for unlocking the utility and updating the utility, wherein the verifying programming is performed by a trusted platform module (TPM) in accordance with Trusted Computing Platform Alliance Specifications.

14. The computer program product as recited in claim 13, wherein the SMI handler used to query the status of the verifying programming queries the TPM for the status.

15. The computer program product as recited in claim 14, wherein the SMI handler is issued by the TPM.

16. The computer program product as recited in claim 13, further comprising:

after the utility has been updated, programming for locking the utility with the SMI handler.

17. The computer program product as recited in claim 13, wherein the requesting programming is performed by an SMI handler.

18. A data processing system comprising:

a processor;

a trusted platform module (TPM) coupled to the processor and operating under Trusted Computing Platform Alliance Specifications;

a BIOS utility stored in flash memory coupled to the processor;

an input circuit for receiving an update to the BIOS utility; and

a bus system for coupling the input circuit to the processor;

a BIOS update application requesting an unlock of the flash memory from a system management interrupt (SMI) handler;

the SMI handler including programming for requesting cryptographic verification of the BIOS utility update from the TPM;

the TPM including programming for verifying an authenticity of the BIOS utility update;

the TPM including programming for issuing an SMI to query the TPM for a status on the verifying of the authenticity of the BIOS utility update;

the SMI handler unlocking the flash memory if the SMI handler sets the status as successful;

the BIOS update application updating the BIOS utility with the update; and

the SMI handler locking the flash memory after the update of the BIOS utility has completed.

19. A method comprising the steps of:

(a) a BIOS update application requesting an unlock of a flash utility from a system management interrupt (SMI) handler;

(b) determining if a verification of an update to the flash utility is pending;

(c) if verification of the update to the flash utility is not pending, the SMI handler requesting verification of the update to the flash utility from a trusted platform module (TPM) and setting a status flag as pending;

(d) exiting the SMI handler and returning status flag to the BIOS update application;

(e) receiving by the BIOS update application the status flag from the SMI handler;

(f) returning to step (a) if the status flag is set as pending after step (e);

(g) in response to step (c), the TPM verifies the update to the flash utility;

(h) when step (g) is completed, issuing an SMI by the TPM to query if the verification of the update to the flash utility was successful or failed;

(i) setting the status flag as successful if the verification of the update to the flash utility was successful;

(j) setting the status flag as failed if the verification of the update to the flash utility was not successful;

(k) if step (b) determines that verification of the update to the flash utility is still pending, determining if the verification of the update to the flash utility has completed;

(l) if step (k) determines that verification of the update to the flash utility has not completed, setting the status flag as pending;

(m) if step (k) determines that verification of the update to the flash utility has completed, determining if the verification of the update to the flash utility was successful;

(n) if step (m) determines that the verification of the update to the flash utility was not successful, setting the status flag as failed;

(o) if step (m) determines that the verification of the update to the flash utility was successful, the SMI handler unlocking the flash utility and setting the status flag as successful;

(p) performing steps (d) and (e) in response to any of steps (l), (n), or (o);

(q) determining if the status flag is set as successful if after step (e) it is determined that the status flag is not set to pending; and

(r) updating the BIOS with the update to the flash utility and locking the flash utility with the SMI handler if the status flag is determined to be set to successful in step (q).

EVIDENCE APPENDIX

No evidence was submitted pursuant to §§1.130, 1.131, or 1.132 of 37 C.F.R. or of any other evidence entered by the Examiner and relied upon by Appellants in the Appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings to the current proceeding.